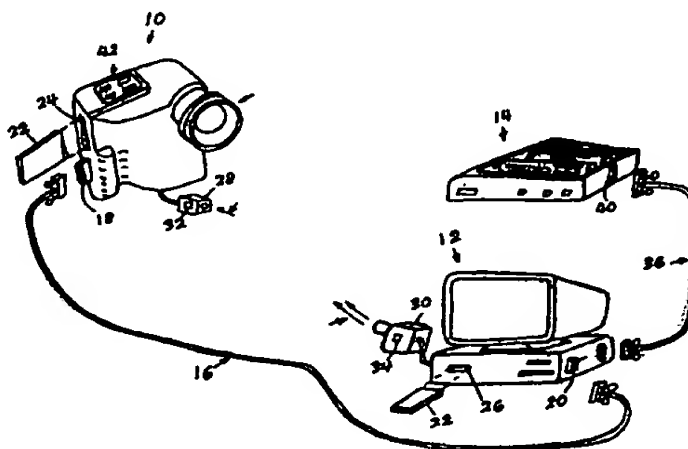




INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁶ : H04N 7/167, 1/44, 5/76, H04K 1/00, H04L 9/00, G09C 3/00		A1	(11) International Publication Number: WO 97/36426
			(43) International Publication Date: 2 October 1997 (02.10.97)
(21) International Application Number: PCT/US97/04993		(81) Designated States: CA, JP, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).	
(22) International Filing Date: 27 March 1997 (27.03.97)		<p>Published</p> <p><i>With international search report.</i></p> <p><i>Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.</i></p>	
(30) Priority Data: 08/623,462 28 March 1996 (28.03.96) US			
(71) Applicant: OBSIDIAN IMAGING, INC. [US/US]; 14255 Amherst Court, Los Altos, CA 94022 (US).			
(72) Inventors: STEINBERG, Eran; 372 Douglas Street, San Francisco, CA 94114 (US). YEREMENKO, Vasily; 121 Saratoga Avenue #4317, Santa Clara, CA 95051 (US).			
(74) Agent: JAFFER, David, H.; Rosenblum, Parish & Isaacs, 15th floor, 160 W. Santa Clara Street, San Jose, CA 95113 (US).			

(54) Title: METHOD AND APPARATUS FOR IN-CAMERA ENCRYPTION



(57) Abstract

A digital camera (10) method and apparatus providing encryption of an image during the acquisition process, and therefore avoiding any state wherein unencrypted image data exists. An encrypted password is generated (70, 80). This is done either by a user and downloaded to the camera, or it is generated in the camera and displayed to the user. Inside the camera, an encryption generator is initialized upon reception and successful decryption of the password (82), whereupon light is admitted from an object to be photographed and converted to digital image data (88). The camera then performs a first encrypting operation (95) on the digital image data to create temporarily encrypted image data. This encrypted data is saved temporarily (96), whereupon it is decrypted in increments (98) and each increment processed to form processed image data. Each increment then undergoes a second and final encryption operation to create final encrypted image data which is stored in the camera for transmission to a computer.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mozambique	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	PL	Poland		
CM	Cameroon	KR	Republic of Korea	PT	Portugal		
CN	China	KZ	Kazakhstan	RO	Romania		
CU	Cuba	LC	Saint Lucia	RU	Russian Federation		
CZ	Czech Republic	LI	Liechtenstein	SD	Sudan		
DE	Germany	LK	Sri Lanka	SE	Sweden		
DK	Denmark	LR	Liberia	SG	Singapore		
EE	Estonia						

1 Specification

2
3 METHOD AND APPARATUS FOR IN-CAMERA ENCRYPTION
45 BACKGROUND OF THE INVENTION
67 Field of the Invention

8 The present invention relates generally to methods and
9 apparatus for encrypting images, and more particularly to a
10 method and apparatus for encrypting images in a camera as part
11 of the image acquisition process.
12

13 Brief Description of the Prior Art

14 The use of encryption techniques to secure messages is
15 well known in history. With modern data communications and
16 storage devices often accessible by third parties, the
17 securing of information is a problem receiving a great deal
18 of attention. For example, in U.S. Patent No. 5,159,630 by
19 Tseng et al. a system for maintaining the security of
20 information transmitted between facsimile machines is
21 described wherein messages on paper are encrypted by the
22 facsimile machine, transmitted in secure encrypted form and
23 decrypted at the receiving end. U.S. Patent 5,420,924
24 discloses a method of encryption using a scanner with digital
25 technology to record an image and then sample and encrypt a
26 portion of it for comparison with an image presented on an
27 I.D. card.

28 In order to secure data transmission, the data is encoded
29 on the sending end and decoded at the receiving end. This
30 deters a third party from deciphering the message in route.
31 Such a method is described in U.S. Patent No. 5,233,653 by
32 Katsurabayashi.

33 A method of securing payment documents is described in
34 U.S. Patent No. 5,297,202 wherein a document is signed by a
35 customer and a copy of the signature is captured in digital
36 form. Thereafter the signature is encrypted and saved along
37 with a digital record of the transaction.

1 In addition to the above methods of achieving secured
2 messages, signatures and I.D. cards, there is a need in the
3 area of conventional digital photography. Images captured and
4 stored by a digital camera on a PCMCIA card, or downloaded to
5 a PC are subject to interception and viewing by unauthorized
6 persons. Typically, a digital camera outputs digital image
7 data to a PCMCIA card, disk, or through lines to a computer.
8 The card or disk could be intercepted and the image viewed,
9 or the data downloaded to a computer could be extracted prior
10 to an encryption procedure. Newspaper reporters,
11 investigators, etc. have a need to temporarily store
12 photographic images in a way that is secure from unauthorized
13 viewing. There is, therefore, a need for a camera that will
14 provide encrypted, secure image data from the moment of image
15 acquisition.

16

17 SUMMARY OF THE INVENTION

18 It is therefore an object of the present invention to
19 provide a camera that encrypts photographic images.

20 It is a further object of the present invention to
21 provide a camera which encrypts a photographic image in the
22 process of image acquisition.

23 It is a still further object of the present invention to
24 provide a camera that does not store or transfer an
25 unencrypted image, even temporarily.

26 Briefly, a preferred embodiment of the present invention
27 includes a digital camera method and apparatus providing
28 encryption of an image during the acquisition process, and
29 therefore avoiding any stage wherein unencrypted image data
30 exists. An encrypted password is generated. This is done
31 either by a user and downloaded to the camera, or it is
32 generated in the camera and displayed to the user. Inside the
33 camera, an encryption generator is initialized upon reception
34 and successful decryption of the password, whereupon light is
35 admitted from an object to be photographed and converted to
36 digital image data. The camera then performs a first
37 encrypting operation on the digital image data to create
38 temporarily encrypted image data. This encrypted data is

1 saved temporarily, whereupon it is decrypted in increments and
2 each increment processed to form processed image data. Each
3 increment then undergoes a second and final encryption
4 operation to create final encrypted image data which is stored
5 in the camera for transmission to a computer. As an
6 alternative to storing the encrypted data temporarily, the
7 camera can process it directly and then encrypt and save it
8 in camera storage. At no stage in the image acquisition
9 process is there a point where image data is stored in
10 unencrypted form on a medium of a type from which unauthorized
11 access can be obtained.

12 An advantage of the present invention is that it provides
13 secure image encryption by performing the encryption as part
14 of the image acquisition, whereas prior art systems allow a
15 step where unencrypted images are readable.

16 A further advantage of the present invention is that in
17 case of a malfunction of the system, any stored image data is
18 encrypted and therefore unreadable.

19 A still further advantage of the present invention is a
20 savings in processing time due to the elimination of the
21 intermediate step of transporting unencrypted images to a
22 computer for encryption.

23

24

IN THE DRAWINGS

25 Fig. 1 illustrates the operation of a camera encryption
26 system according to the present invention;

27 Fig. 2 is a block diagram showing the major components
28 of a digital camera;

29 Fig. 3 is a block diagram describing the programmed
30 operations of the digital camera encryption system of the
31 present invention and its use with a host computer and printer;

32 Fig. 4 is a block diagram detailing the steps involved
33 in encrypting; and

34 Figs. 5A and 5B are tables with data illustrating a
35 simple example of the basic concept of digital encryption.

36

37

1 DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

2 Referring now to Fig. 1 of the drawing, there is an
3 illustration of the operation of a camera encryption system
4 according to the present invention. There is a digital camera
5 10, a host computer 12 and a printer 14. A variety of means
6 of communication between the camera 10 and computer 12 are
7 shown including a cable assembly 16 interconnecting with the
8 camera 10 and computer 12 through connectors 18 and 20.
9 Communication can also be accomplished through use of a disk
10 22, such as a PCMCIA card for use with card/disk slots 24, 26.
11 Radiated signals can also be used for communication as
12 indicated by transceivers 28, 30. In addition, information
13 can also be transferred through connections 32, 34 to a modem
14 for transmission through a telephone system. The computer 12
15 is shown interconnected with the printer 14 by way of cable
16 assembly 36 and connector 38, 40.

17 The camera 10 is constructed and configured for
18 encrypting images as part of the image acquisition process.
19 The process begins with either the user or camera 10 supplying
20 a password, the choice being made by the user through
21 operation of a camera control located, for example, on camera
22 control and display 42. The operator can prepare the password
23 in encrypted form through the use of the computer 12, the
24 password then being downloaded to the camera through any of
25 the communication methods described above. Alternatively, the
26 user can choose from controls provided to have the camera 10
27 supply and display a password for example on the control and
28 display 42.

29 In response to receiving an encrypted password, the
30 camera 10 initializes an encryption generator, and then in
31 response to user activation takes the picture. According to
32 the present invention, the camera 10 then acquires an image
33 and converts it to digital data. This data is then handled
34 in one of two ways. One of these is to process it directly
35 to create processed image data and thereafter encrypt it to
36 form final encrypted image data. Alternatively, according to
37 the preferred embodiment of the present invention, and
38 providing enhanced security, the image data can undergo a

1 first encryption to create temporarily encrypted image data
2 which can be safely stored in the camera. This temporarily
3 encrypted data is then extracted in increments, and each
4 increment is decrypted and processed to form an increment of
5 processed image data, which then undergoes a second and/or
6 final encryption to form final encrypted image data. The
7 advantage of this procedure is that when the raw data is
8 initially encrypted prior to processing, there is no step in
9 the camera process wherein any unencrypted data is stored, and
10 therefore it is more secure against an unauthorized attempt
11 to acquire the image data.

12 Following the camera image acquisition process, the final
13 encrypted data is sent to the computer 12 by any of the means
14 described above, whereupon the image can be viewed or printed
15 (printer 14) upon user presentation of the password.

16 Fig. 2 shows a block diagram of the major operational
17 portions of a digital camera. These include an image
18 acquisition apparatus 44 in communication through bus 46 with
19 a processor 48. The processor by way of bus 52, stores data
20 in memory 50, which also includes memory for basic operations,
21 the memory also referred to as an image buffer. Input and
22 output of data is through one of the various means described
23 above, including a cable connector 54 through bus 56,
24 card/disk slot 58 through bus 60, transceiver 62 by way of bus
25 64, or modem connection (not shown in Fig. 2). Controls 42
26 are shown connected to the processor by way of bus 66.

27 The image acquisition apparatus 44 includes components
28 well known by those skilled in the art and need not be shown
29 in detail in order to practice the invention. The acquisition
30 apparatus 44 includes an image optical pickup such as a
31 charged coupled device (CCD) and A/D circuitry to convert the
32 analog CCD signals to digital form for the processor 48.

33 Referring now to Fig. 3, an operational block diagram
34 details the encryption process of the present invention. The
35 blocks of Fig. 3 include the novel camera operations and the
36 operations performed by the associated host computer system.
37 Blocks 70 and 72 illustrate the two methods of determining the
38 password described above. According to block 70, the operator

1 creates a password through use of the host computer 12. This
2 can be done either manually, the user providing the password
3 (block 74), or the operator can instruct the host computer 12
4 to create a password (block 76). In either case, the host
5 computer is programmed to encrypt the password (block 78)
6 prior to downloading (block 80) to the first camera 10
7 operation (block 82). Alternatively, the camera 10 can
8 provide the password, as indicated in block 72, beginning with
9 the camera 10 generating a password 84 according to pre-
10 programmed guidelines. The password is then displayed for the
11 user to make record of and encrypted (block 86). The
12 encrypted password is then sent to block 82. The above
13 password encryption process describes and employs a single
14 password for initializing the camera to take a picture and
15 encrypt an image, as well as for decrypting the encrypted
16 image at a later stage, such as in the host computer after the
17 encrypted image data has been transferred to the computer.
18 Another alternate password method is to use one password for
19 encrypting the image, and another for decrypting it. A
20 further alternative would be to not require a password at all
21 for encryption, but only for decryption. Such would be the
22 case in what is called a public/private key. These
23 alternatives are included in the present invention.

24 The camera 10 operation of picture taking proceeds
25 according to block 82 by decrypting the password, checking its
26 validity and initializing/initiating the encryption process.
27 If the password is correct, the picture is "taken" (block 88).

28 The camera functions of handling the password as
29 described above are directed by the processor 48 in
30 communication with the operator controls 42 and memory 50.
31 The process of "taking" the picture (block 88) involves the
32 image acquisition circuitry 44 as explained above. The
33 processor 48 upon receipt of the digital image data can then
34 proceed with the image processing and encrypting in one of the
35 two ways according to the particular system programming or
36 user selection. The choice of particular method of
37 processing, i.e. the image data stored in unencrypted or
38 encrypted form internal to the camera, is made by either hard

1 wire in the camera or as an alternative, selectable through
2 an operator control 42 on the camera.

3 If the greatest degree of security is required, the
4 camera is programmed to proceed to provide a temporary
5 encryption of the raw image data supplied by the image
6 acquisition apparatus 44. This choice is indicated by
7 arrow/path 90 and the temporary (ephemeral) encryption is
8 performed according to block 92, beginning with the generation
9 of a temporary encryptor or i.e. key, (block 94) which is
10 processed with the raw data via line 90 to create temporary
11 encrypted data (block 95) which is saved in memory 50 as
12 indicated by block 96. This temporary or i.e. first
13 encryption avoids the need to save unencrypted data, and
14 provides added security in that there is no data storage from
15 which an unauthorized user could extract unencrypted data even
16 if the camera is in the possession of an unauthorized
17 individual. The temporary saving of data (block 96) is needed
18 when/if the processor 48 can not handle all of the incoming
19 data immediately. The processor 48 then extracts the
20 encrypted data in increments, each increment of data decrypted
21 (block 98) and processed (block 100) to form processed image
22 data.

23 The temporary encryptor of block 94 is initialized by an
24 internal password. This password can be different from the
25 password available to the operator as discussed above in
26 reference to blocks 70, 72, and different from a password
27 associated with block 112 to be described in the following
28 specification in relation to decrypting image data at a host
29 computer. The present invention includes an alternate
30 embodiment wherein the internal password is different from the
31 first password for encrypting or i.e., taking the picture, and
32 different from a second password for decrypting the final
33 encrypted image data, which can be the same password as or
34 different from the first password. The programming according
35 to the present invention includes the alternative of the
36 camera randomly selecting an internal password, and also
37 selecting a different internal password each time data is
38 temporarily encrypted. This process makes it impossible for

1 anyone to extract unencrypted data from internal camera
2 storage.

3 Following the temporary encryption and/or processing of
4 the image data, the processed image data then undergoes a
5 second or i.e. final encryption and storage (block 102).
6 Block 102 shows the second/final encryption (block 104), and
7 saving of the final encrypted image data (block 106) in the
8 camera memory, or removable external storage device 50. Upon
9 user command through controls 42, the camera 10 transmits the
10 final encrypted image data (block 108) to the host computer
11 12 (block 110). In order to use the image data, the password
12 is presented by the user (block 112) and the data is decrypted
13 (block 114). Again, the camera encryption programming can be
14 done so that the password required at this point can be
15 different from or the same as the password to encrypt. At
16 this point the user can view the image 116, print the image
17 118, or/and save the image 120.

18 In order to clarify a process of digital encryption of
19 data, a simplified example is now given with the assistance
20 of Figs. 4, 5A and 5B. To begin with, upon reception of a
21 correct password (block 122) the processor 48 creates a key
22 (block 124) of a predetermined length K. An input data stream
23 (block 126) of length N is loaded K bits at a time (block 128)
24 and exclusive OR'd (XOR'd) with the key (block 130). The
25 result of the XOR block 130 is stored (block 132), and while
26 the input stream lasts (block 134), another length of K bits
27 is loaded (block 128). The XOR'd image stream is returned,
28 i.e. stored as encrypted data in memory 50 (block 136).

29 Figs. 5A and 5B illustrate a simple example of the
30 processes of encryption and decryption using all possible
31 combinations of the binary XOR operation. The key length in
32 the example is K=4 and equal to 1010 (column 138). Fig. 5A
33 shows the process of encryption. An image data stream is
34 assumed to have an incremental length of 4 data bits equal to
35 1100 (column 140). The first row 141 shows a "1" bit of image
36 data XOR'd with a "1" bit of the key to yield a "0" result
37 because of the "exclusive OR" function. Similarly, "1" XOR'd
38 with "0" results in "1", as does "0" XOR'd with "1", and "0"

1 XOR'd with "0" in the next two rows yields "0", the results
2 all shown entered in column 142. Similarly, Fig. 5B shows the
3 process of decryption, the image data (column 144) being the
4 encrypted "result" from Fig. 5A, which is XOR'd with the key
5 (column 146) to yield the decrypted original data in column
6 148 which is exactly the same as column 140 in Fig. 5A as it
7 should be.

8 Referring again to Fig. 4, a more lengthy example is
9 given in blocks 150-160, where block 150 contains the input
10 data stream and block 152 the key. Block 154 contains the
11 first 8 bits of the stream in block 150 loaded according to
12 block 128. Block 156 shows the first 8 bits XOR'd with the
13 key of block 152. Block 158 indicates the first
14 XOR'd/encrypted bits stored. Block 160 is the final encrypted
15 complete data stream.

16 Although the use of an XOR function is described for
17 encrypting, other functions or formulas can be used to
18 transform/encrypt digital data from an original to a coded
19 form, with the reverse process being performed for decryption.
20 These various alternate functions and formulas are also
21 included in the spirit of the present invention when used for
22 in-camera encryption.

23 Although a preferred embodiment of the present invention
24 has been described above, it will be appreciated that certain
25 modifications or alternations thereon will be apparent to
26 those skilled in the art. It is therefore requested that the
27 appended claims be interpreted as covering all such
28 alterations and modifications that fall within the true spirit
29 and scope of the invention.

30

1 What is claimed is:

CLAIMS

1 1. A method of secure processing of digital image data in
2 a digital camera system, said method comprising:

3 a) converting light to digital image data; and

4 b) encrypting within said camera said digital image data
5 to final encrypted image data.

1 2. A method as recited in claim 1 wherein said encrypting
2 includes

3 a) first encrypting said digital image data to
4 temporarily encrypted image data;

5 b) saving said temporarily encrypted image data;

6 c) decrypting said temporarily encrypted image data to
7 form decrypted image data;

8 d) processing said decrypted image data to form processed
9 image data; and

10 e) second encrypting said processed image data to form
11 said final encrypted image data.

1 3. A method as recited in claim 1 wherein said encrypting
2 includes

3 a) processing said image data; and

4 b) final encrypting said image data to form said final
5 encrypted image data.

1 4. A method as recited in claim 2 wherein

2

3 a) said decrypting said temporarily encrypted image data
4 includes decrypting incremental quantities of said temporarily
5 encrypted image data to form quantities of incremental
6 decrypted image data; and

7 b) said processing said decrypted image data includes
8 processing each of said quantities of incremental decrypted
9 image data to form said processed image data.

1 5. A method as recited in claim 1 wherein said encrypting
2 is initialized in response to a password.

1 6. A method as recited in claim 5 further comprising:

2 a) generating a password; and

3 b) communicating said password to a camera user.

1 7. A method as recited in claim 5 further comprising:

2 a) receiving said password as an encrypted password from
3 a source external to said camera; and

4 b) decrypting said encrypted password to form said
5 password.

1 8. A method as recited in claim 1 further comprising:

2 a) saving said final encrypted image data; and

3 b) transmitting said final encrypted image to a device
4 external to said camera.

1 9. A method of encrypting digital image data in a camera,
2 said method comprising:

- 3 a) converting light to digital image data; and
4 b) encrypting within said camera said digital image data
5 to final encrypted image data.

1 10. A method as recited in claim 9 wherein said encrypting
2 includes

- 3 a) first encrypting said digital image data to
4 temporarily encrypted image data;
5 b) saving said temporarily encrypted image data;
6 c) decrypting said temporarily encrypted image data to
7 form decrypted image data;
8 d) processing said decrypted image data to form processed
9 image data; and
10 e) second encrypting said processed image data to form
11 said final encrypted image data.

1 11. A method as recited in claim 9 wherein said encrypting
2 includes

- 3 a) processing said image data; and
4 b) final encrypting said image data to form said final
5 encrypted image data.

1 12. A method as recited in claim 10 wherein

- 2 a) said decrypting said temporarily encrypted image data
3 includes decrypting incremental quantities of said temporarily

4 encrypted image data to form quantities of incremental
5 decrypted image data; and

6 b) said processing said decrypted image data includes
7 processing each of said quantities of incremental decrypted
8 image data to form said processed image data.

1 13. A method as recited in claim 9 wherein said encrypting
2 is initialized in response to a password.

1 14. A method as recited in claim 13 further comprising:

2 a) generating a password; and

3 b) communicating said password to a camera user.

1 15. A method as recited in claim 13 further comprising:

2 a) receiving said password as an encrypted password from
3 a source external to said camera; and

4 b) decrypting said encrypted password to form said
5 password.

1 16. A method as recited in claim 9 further comprising:

2 saving said final encrypted image data in said camera for
3 transmission to a device external to said camera.

1 17. A camera for securely processing image data comprising:

2 a) means for converting light to digital image data; and

3 b) means for encrypting within said camera said digital
4 image data to final encrypted image data.

1 18. A camera as recited in claim 17 wherein said means for
2 encrypting includes

3 a) means for first encrypting said digital image data to
4 temporarily encrypted image data;

5 b) means for saving said temporarily encrypted image
6 data;

7 c) means for decrypting said temporarily encrypted image
8 data to form decrypted image data;

9 d) means for processing said decrypted image data to form
10 processed image data; and

11 e) means for second encrypting said processed image data
12 to form said final encrypted image data.

1 19. A camera as recited in claim 17 wherein said means for
2 encrypting includes

3 a) means for processing said image data; and

4

5 b) means for final encrypting said image data to form
6 said final encrypted image data.

1 20. A camera as recited in claim 18 wherein

2 a) said means for decrypting said temporarily encrypted
3 image data includes means for decrypting incremental
4 quantities of said temporarily encrypted image data to form
5 quantities of incremental decrypted image data; and

6 b) said means for processing said decrypted image data
7 includes means for processing each of said quantities of

8 incremental decrypted image data to form said processed image
9 data.

1 21. A camera as recited in claim 17 wherein said means for
2 encrypting is initialized in response to a password.

1 22. A camera as recited in claim 21 further comprising:
2 a) means for generating a password; and
3 b) means for communicating said password to a camera
4 user.

1 23. A camera as recited in claim 21 further comprising:
2 a) means for receiving said password as an encrypted
3 password from a source external to said camera; and
4 b) means for decrypting said encrypted password to form
5 said password.

1 24. A camera as recited in claim 17 further comprising:
2 a) means for saving said final encrypted image data; and
3 b) means for transmitting said final encrypted image to
4 a device external to said camera.

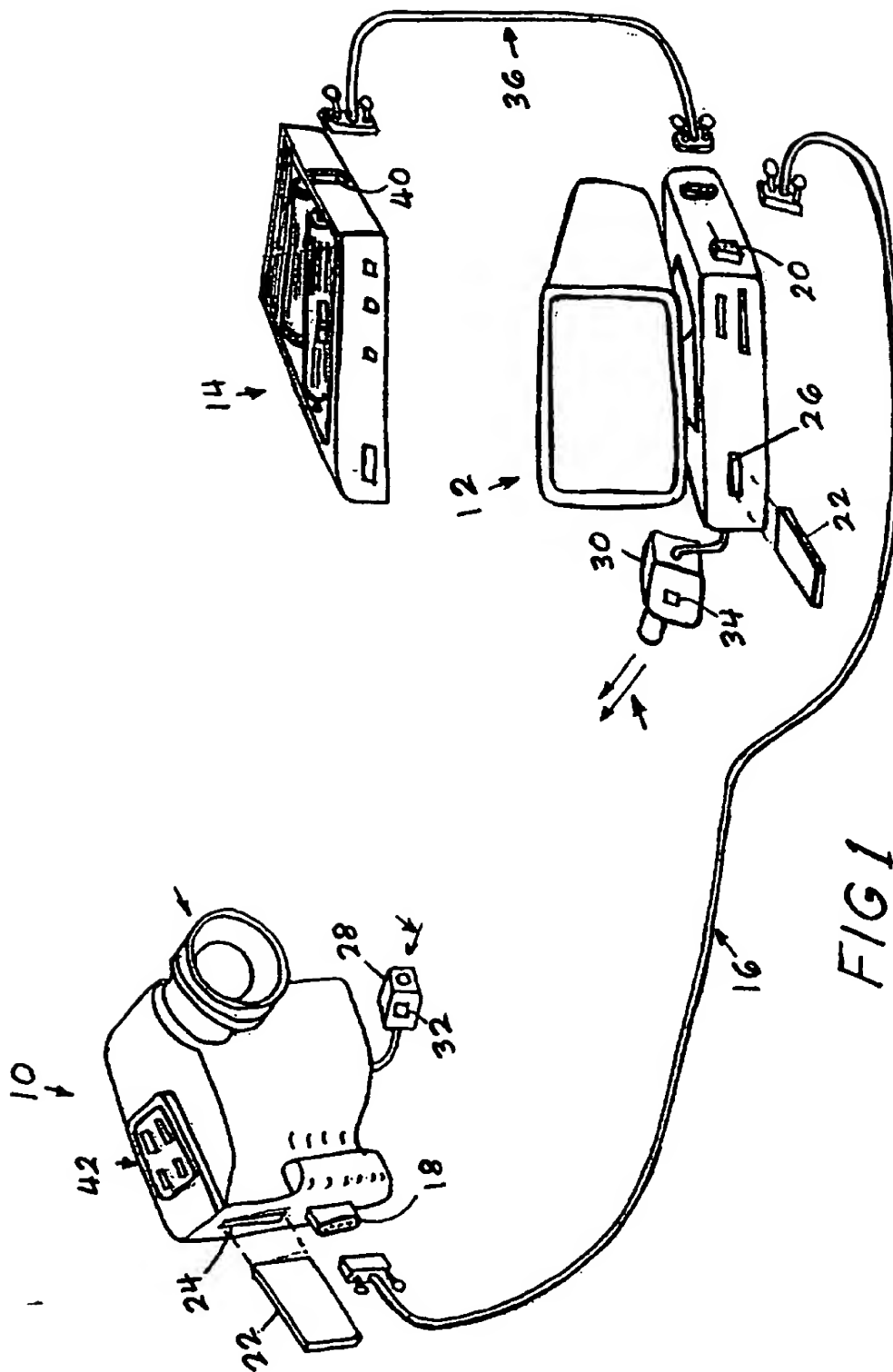
1 25. A method as recited in claim 2 further comprising:
2 creating within said camera a randomly generated internal
3 password required in order to accomplish said first encrypting
4 and said decrypting said temporarily encrypted image data.

1 26. A method as recited in claim 9 further comprising:

2 creating within said camera a randomly generated internal
3 password required in order to accomplish said first encrypting
4 and said decrypting said temporarily encrypted image data.

1 27. A camera as recited in claim 18 further comprising:
2 means for creating within said camera a randomly
3 generated internal password required in order to initiate said
4 means for first encrypting and said means for decrypting said
5 temporarily encrypted image data.

1/5



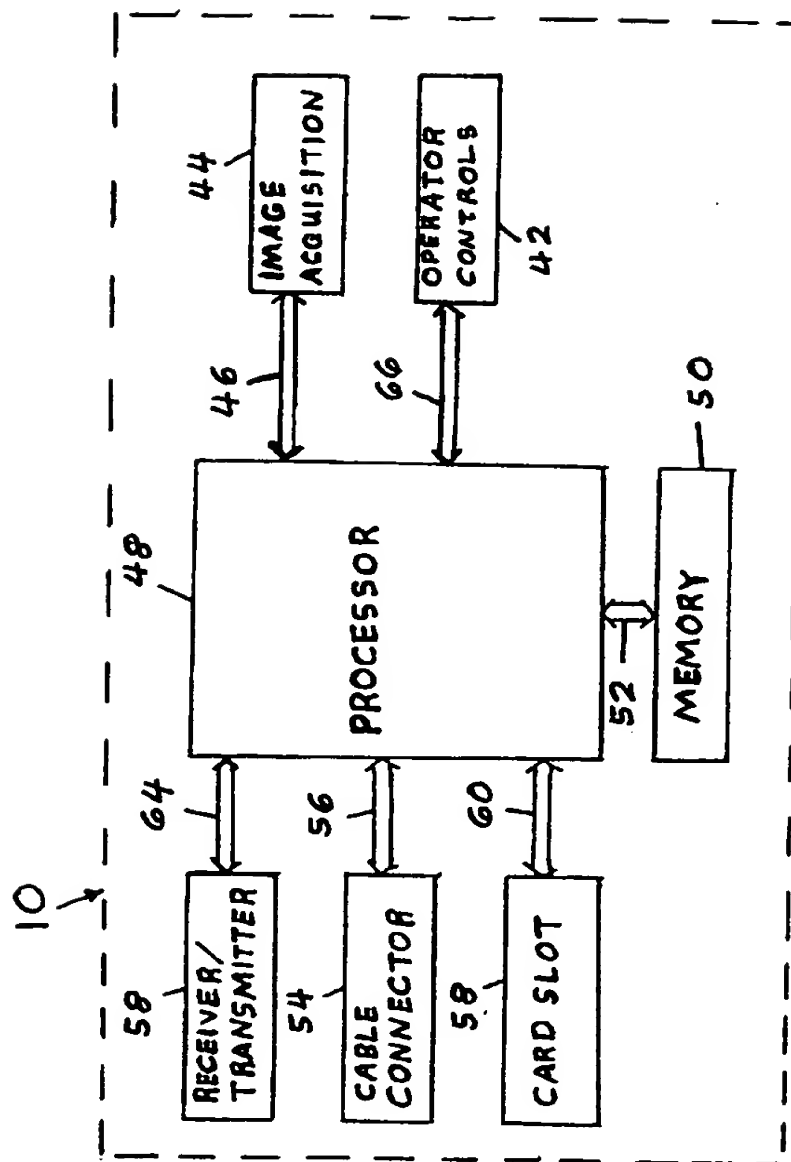
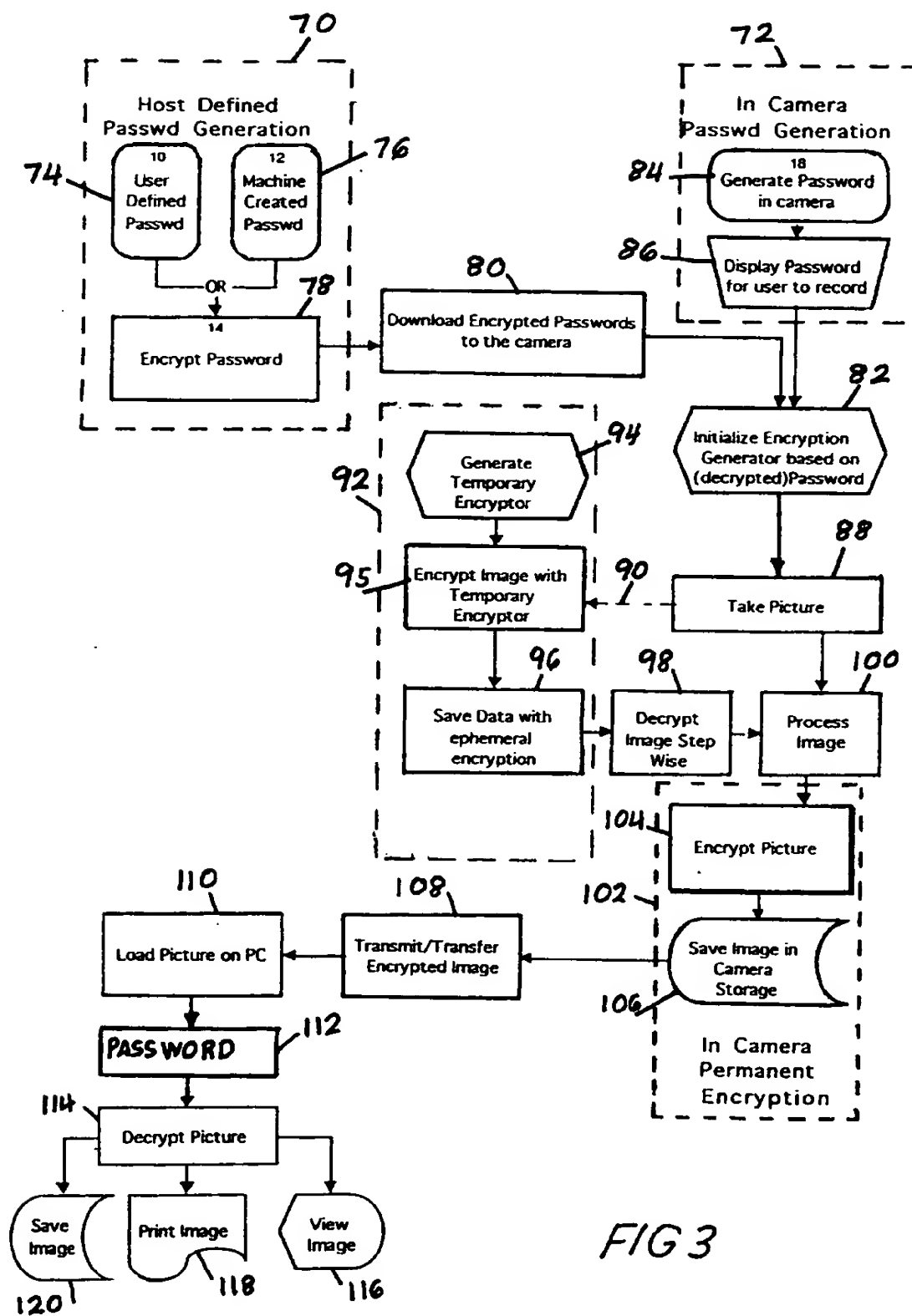


FIG 2

3/5



4/5

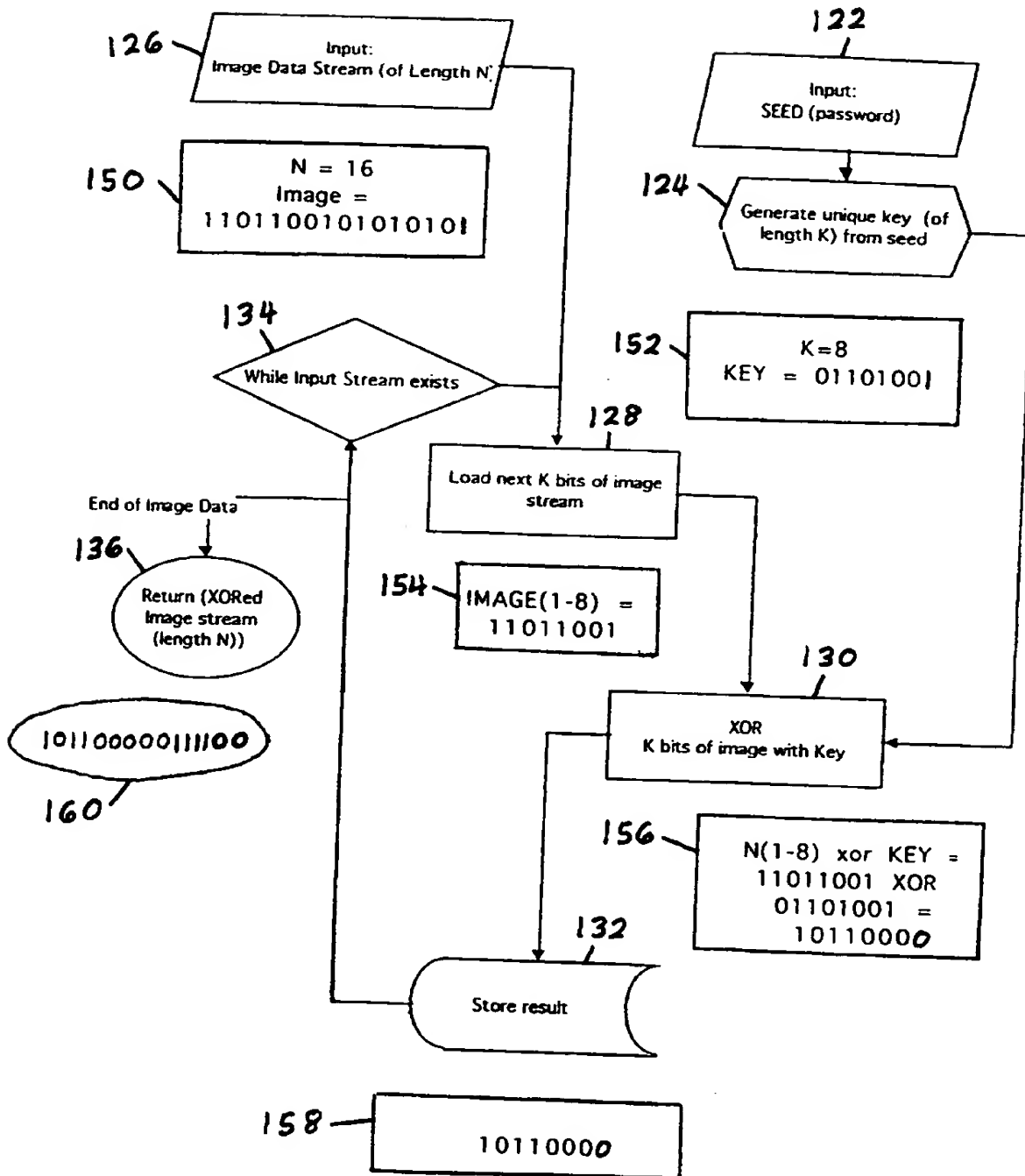


FIG 4

	140 ↓	138 ↓	142 ↓
	Image	Key	Result
141 →	1	1	0
143 →	1	0	1
	0	1	1
	0	0	0

FIG 5A

148 ↓	146 ↓	144 ↓
Result	Key	Image
1	1	0
1	0	1
0	1	1
0	0	0

FIG 5B

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US97/04993

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) : H04N 7/167, 1/44, 5/76; H04K 1/00; H04L 9/00; G09C 3/00

US CL : 380/10, 18, 23, 54; 348/231, 233, 552

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/10, 18, 23, 54; 348/231, 233, 552

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

APS Messenger

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US, A, 5,499,294(FRIEDMAN) 12 March 1996, see entire document.	1, 3, 8, 9, 11, 16, 17, 19, 26
A, P	US, A, 5,581,613 (NAGASHIMA ET AL) 03 December 1996.	1-27
A	US, A, 5,468,587 (COE ET AL) 21 November 1995.	1-27
A	US, A, 5,430,525 (OHTA ET AL) 04 July 1995.	1-27
A	US, A, 5,420,924 (BERSON ET AL) 30 May 1995.	1-27
A	US, A, 5,410,642 (HAKAMATSUKA) 25 April 1995.	1-27
A	US, A, 5,301,444 (WRIGHT) 05 April 1995.	1-27

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" documents defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier document published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"A" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search

03 JULY 1997

Date of mailing of the international search report

05 AUG 1997

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231

Facsimile No. (703) 305-3230

Authorized officer

Stephen C. Buczinski
STEPHEN C. BUZINSKI

Telephone No. (703) 305-1835

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US97/04993

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US, A, 5,384,846 (BERSON ET AL) 24 January 1995.	1-27
A	US, A, 5,355,411 (MACDONALD) 11 October 1994.	1-27
A	US, A, 5,337,362 (GORMISH ET AL) 09 August 1994.	1-27
A	US, A, 5,303,370 (BROSH ET AL) 12 April 1994.	1-27
A	US, A, 5,297,202 (KAPP ET AL) 22 March 1994.	1-27
A	US, A, 5,204,901 (HERSHEY ET AL) 20 April 1993.	1-27
A	US, A, 5,027,401 (SOLTESZ) 25 June 1991.	1-27